What is claimed is:

1. A public, non-commutative method for encoding an original message to be passed to a recipient by way of an grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor;

generating a public proxy key based on a private key corresponding to the recipient, wherein it is computationally difficult to recover the private key corresponding to the recipient from the public proxy key; and

applying the public proxy key to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and any available public information.

2. The method of claim 1, wherein the encrypted message has been encrypted with an ElGamal encryption scheme.

3. The method of claim 1, wherein the encrypted message has been encrypted with a modified ElGamal encryption scheme.

4. The method of claim 1, wherein the receiving, generating, and applying steps are performed by the grantor.

5. The method of claim 1, further comprising the step of providing the transformed message to the recipient.

6. The method of claim 5, further comprising the step of decrypting the transformed message using information selected from the private key corresponding to the recipient and any available public information.

7. The method of claim 5, further comprising the step of decrypting the transformed message using the private key corresponding to the recipient.

8. The method of claim 2, wherein the encrypted message comprises a first portion and a second portion, the first portion encoding a generator and a random key, and the second portion encoding the original message, the public key corresponding to the grantor, and the random key.

9. The method of claim 8, wherein the applying step operates on the second portion of the encrypted message.

10. The method of claim 3, wherein the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key.

11. The method of claim 10, wherein the applying step operates on the second portion of the encrypted message.

12. The method of claim 4, wherein the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key.

13. The method of claim 12, wherein the applying step operates on the second portion of the encrypted message.

14. The method of claim 1, wherein the original message is passed to a recipient through at least one additional intermediate grantor by repeating the generating and applying steps for each additional intermediate grantor.

15. A public, non-commutative method for encrypting an original message to be passed to a recipient by way of an grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor; and

transforming the encrypted message, using a transformation key corresponding to the recipient, into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from a private key corresponding to the recipient and any available public information.

16. The method of claim 15, wherein the transformation key comprises a private key corresponding to the recipient.

17. The method of claim 15, wherein the transformation key comprises a public key corresponding to the recipient.

18. The method of claim 15, wherein the encrypted message has been encrypted with a Cramer-Shoup encryption scheme.

19. The method of claim 15 wherein the transformed message is decryptable by the recipient using a private key corresponding to the recipient.

20. The method of claim 15, wherein the original message is passed to a recipient through at least one additional intermediate grantor by repeating the transforming step for each additional intermediate grantor.